NATIONAL AERONAUTICS AND SPACE ADMINISTRATION
COUNTERINTELLIGENCE CYBER (CI CYBER)

CI CYBER TALK

VOLUME 2, ISSUE 2 **AUGUST 2017**

This Issue

- Under Pressure, Western Tech Firms Bow to Russian Demands to Share Cyber Secrets
- 10 Cyber Security Threats for 2017 Everyone Should Know About
- How One Typo Helped Let Russian Hackers In
- Kaspersky Lab Has Been Working With Russian Intelligence
- DIA Reveals New Details of Russian Information Warfare
- Hacking the State of the ISIS Cyber Caliphate
- Your Guide to Russia's Infrastructure Hacking Teams

NATIONAL AERONAUTICS AND SPACE ADMINISTRATION,
COUNTERINTELLIGENCE
DARRELL SLONE, NASA CI DIRECTOR
DARRELL.D.SLONE@NASA.GOV

DISTRIBUTION

NASA CI distributes the CI Cyber Talk to NASA ITSEC, OCIO, and other employees with an official need for the information.
NASA CI will not distribute this product to personal email accounts (e.g., @yahoo.com, etc.).

CI CYBER TALK

VOLUME 2, ISSUE 2 **AUGUST 2017**

The purpose of this product is to inform readers about possible exploitation, compromise, or illegal acquisition of sensitive or classified U.S. information and technology.

The use of the linked news articles in this publication does not constitute or imply an official endorsement of the content of these articles or of any news organization or media outlet. Further reproduction or distribution of any linked news article appearing in this publication is subject to original copyright restrictions.

Under Pressure, Western Tech Firms Bow to Russian Demands to Share Cyber Secrets

Russian authorities are asking Western tech companies to allow them to review source code for security products such as firewalls, anti-virus applications and software containing encryption before permitting the products to be imported and sold in the country.

Date: June 23, 2017; Source: http://www.reuters.com/article/us-usa-russia-tech-idUSKBN19E0XB

10 Cyber Security Threats for 2017 Everyone Should Know About

The top 10 cyber security concerns that also have a CI concern are as follows; Internet of Things (IoT), ransomware, phishing, social media, public Wi-Fi, 'Support' Scammers, fraudulent email, bad apps, passwords, old hard drives. These cyber security concerns can affect NASA employees working from a NASA center or teleworking; especially if the agency VPN is not used.

Date: May, 2017; Source: https://www.shredit.com/en-us/blog/securing-your-information/may-2017/10-cyber-security-threats-for-2017-everyone-should

How One Typo Helped Let Russian Hackers In

A simple "typo" enabled hackers to compromise and exploit the DNC network.

Date: June 27, 2017; Source: http://www.cnn.com/2017/06/27/politics/russia-dnc-hacking-csr/index.html

CI CYBER TALK

VOLUME 2, ISSUE 2 AUGUST 2017

Kaspersky Lab Has Been Working With Russian Intelligence

US national security officials are starting to become concerned about the company's links to the Russian government.

Date: July 11, 2017; Source: https://www.bloomberg.com/news/articles/2017-07-11/kaspersky-lab-has-been-working-with-russian-intelligence

DIA Reveals New Details of Russian Information Warfare

According to a new Defense Intelligence Agency report, Russian military forces are using information warfare tools to confront the United States.

Date: July 7, 2017; Source: http://freebeacon.com/national-security/dia-reveals-new-details-russian-information-warfare/

Hacking the State of the ISIS Cyber Caliphate

The cyber terrorist group's denial-of-service attack MO is akin to a crowdsourced attack not unlike Anonymous employed in its heyday, for instance. "Their denial-of-service attacks are being executed through Windows applications on multiple hosts, but not infected" bots or a botnet infrastructure. They're mostly using their own, or supporters', machines to pummel websites with SYN or other flood attacks, for example.

Date: July 6, 2017; Source: http://www.darkreading.com/perimeter/hacking-the-state-of-the-isis-cyber-caliphate-/d/d-id/1329293

Your Guide to Russia's Infrastructure Hacking Teams

Russian hackers targeted more than a dozen American energy utilities, including a Kansas nuclear power plant.

Date: July 7, 2017; Source: https://www.wired.com/story/russian-hacking-teams-infrastructure/

CI CYBER TALK
VOLUME 2, ISSUE 2 AUGUST 2017

NASA CENTER COUNTERINTELLIGENCE POC CONTACT LIST

Ames Research Center: Christopher Knoth, 650-604-2250

Armstrong Flight Research Center: Frank Sutton, 661-276-7476

Glenn Research Center: George Crawford, 216-433-8458

Goddard Space Flight Center: Christian Breil, 301-286-1533

Jet Propulsion Laboratory: John J. O'Malley, 818-354-7828

Johnson Space Center: Tony Dietsch, 281-483-7921

Kennedy Space Center: Ron Storey, 321-867-2568

Langley Research Center: Benjamin Marchione, 757-864-3403

Marshall Space Flight Center: Ronald Smith, 256-544-7808

NASA Headquarters: Art Payton, 202-358-4645

Stennis Space Center: David Malcom, 228-688-1683